Clean version of amended claims

1. A method for duplicating information in an IP packet with the intention of using it to partially or completely reverse the effect of intermediate NATs, comprising the steps of:

Identifying parts of an IP packet, including but not limited to the IP and transport layer headers, that can be potentially modified by NATs;

Copying that information into the packet in its current form or copying it into a different format;

Inserting the duplicate information into an IP packet after the IP and transport headers or appending it after the data portion of the packet in an encoded or original form to keep it protected from intermediate NATs.

2. The method of claim 1 wherein complete IP header and the transport layer header is inserted into the IP packet such that the transmitted packet will have duplicate IP and transport layer headers or a duplicate IP or transport layer header.

3. The method of claim 1, wherein the duplicate information is inserted into the IP packets of the same connection using a keyed or keyless encoding to keep it protected from intermediate NATs and recomputing the length and checksum fields in the IP and transport layer headers.

4. The method of claim 1, wherein the duplicate information is inserted into the IP packets of a different connection and there are identifiers inserted into the IP packets of both connections to correlate the information and observe the effect of intermediate NATs.

5. A method for studying the effect of intermediate NATs with the purpose of using it to partially or completely reverse the effect of intermediate NATs, comprising the steps of:

Identifying parts of an IP packet, including but not limited to the transport and IP headers of the packet, that can be potentially modified by intermediate NATs;

Identifying parts of an IP packet from same or different connections that contain the original information, including but not limited to the IP and transport layer headers, before intermediate NATs modified it;

Generating a look-up table that signifies the effect of intermediate NATs on the IP packets of that connection.

6. A method for reversing partially or fully the effect of intermediate NATs based on a look-up table that signifies the effect of NATs on the IP packets of that connection, comprising the steps of:

Modifying the body of the packet that may contain IP address or port numbers modified by intermediate NATs to their original values;

Modifying the transport header by replacing the original port numbers and recomputing part or all of the transport header as necessary;

Modifying the IP header the replacing the original source and destination IP address and recomputing the length and/or checksum.

7. The method of claim 6 wherein only the effect of NAT on the transport layer header is reversed by replacing the modified port numbers with the original ports numbers, adjusting the sequence and acknowledge numbers to correctly reflect the unmodified packet, and recomputing the checksum field.

8. The method of claim 6 wherein only the effect of NAT on the IP header is reversed by replacing the observed source and destination IP address with original source and destination IP addresses followed by recomputation the length and checksum.

9. The method of claim 6 wherein the effect of NAT on the transport layer data is reversed by reverting back to the original port numbers in the transport header, adjusting the sequence and acknowledge numbers if necessary, recomputing the checksum and length fields.

10. A method for correcting the information in outgoing IP packets so that they arrive in a state expected by the NATs comprising the steps of:

Modifying the transport header based on a lookup table so that the port numbers match that of the incoming network connection before the effect of the NAT were reversed;

Modifying the IP header based on a lookup table so that the source and destination IP addresses numbers match that of the incoming network connection before the effect of the NAT were reversed;

Modifying the message body based on a lookup table.

11. The method of claim 10 where IP header and/or the transport header of the outgoing packet is modified by changing the destination and/or source IP headers of the packet based on a lookup table and recomputing the length, checksum, address, port number, sequence, and acknowledge number fields.

12. The method of claim 10 where IP address or port number embedded inside the packet body are modified based on a lookup table and recomputing the length and/or checksum fields in the transport and/or IP headers.